UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/577,507	04/27/2006	John Leach	5035-244US/P32,272 USA	5364

20802 7590 12/08/2009

FOX ROTHSCHILD LLP
P O BOX 592
112 NASSAU STREET
PRINCETON, NJ 08542-0592

EXAMINER	
HAILU, TESHOME	
ART UNIT	PAPER NUMBER
2434	

MAIL DATE	DELIVERY MODE
12/08/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/577,507	LEACH, JOHN	
	Examiner	Art Unit	
	TESHOME HAILU	2434	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 April 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-54* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-54* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 April 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 55-64 have been cancelled.

2. Claims 1-54 are pending.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claims 1-54 are rejected under 35 U.S.C. 101 based on Supreme Court precedent and recent Federal Circuit decisions, a 35 U.S.C § 101 process must (1) be tied to a particular machine or (2) transform underlying subject matter (such as an article or materials) to a different state or thing. In re Bilski et al, 88 USPQ 2d 1385 CAFC (2008); Diamond v. Diehr, 450 U.S. 175, 184 (1981); Parker v. Flook, 437 U.S. 584, 588 n.9 (1978); Gottschalk v. Benson, 409 U.S. 63, 70 (1972); Cochrane v. Deener, 94 U.S. 780,787-88 (1876).

An example of a method claim that would not qualify as a statutory process would be a claim that recited purely mental steps. Thus, to qualify as a § 101 statutory process, the claim should positively recite the particular machine to which it is tied, for example by identifying the apparatus that accomplishes the method steps, or positively recite the subject matter that is being transformed, for example by identifying the material that is being changed to a different state.

Here, applicant's method steps are not tied to a particular machine and do not perform a transformation. Thus, the claims are non-statutory.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 1-54 are rejected under 35 U.S.C. 102(b) as being anticipated by Schneier et al (Schneier) (US 5,850,516).

As per claim 1 Schneier discloses:

A method used in the control of a physical system, comprising the steps of modelling a risk chain, the risk chain being a series of two or more entities that each model a discrete part of how a threat leads to damage to a target system, (column 1, line 6-10, the method and apparatus of the present invention relate generally to electronically analyzing the security of systems and, more particularly, to evaluating the security of an information system against unauthorized attack) and (abstract, line 1-8, a computer-implemented method and apparatus electronically represent and quantify the security of a system as a logical tree structure including leaf nodes representing attacks against the system and intermediate nodes representing various logical combinations of attacks necessary to mount a successful overall attack. An indication of the overall security of the system is quantified in a value of a root node of the tree).

Each entity being described as a population of elements distributed in a parameter or parameters, each entity generating the next entity in the chain; and controlling the physical system by using results of the modelling (column 4, line 53-58, processing software and hardware within computer system 200 then calculate the tree's intermediate nodes and resultant root node value. Thus, the invention transforms information process parameters (leaf node values) into an overall representation of the security of the system).

Claim 28 is rejected under the same reason set forth in rejection of claim 1:

As per claim 2 Schneier discloses:

The method of Claim 1 in which the way one entity in the risk chain generates another entity in the risk chain is described by a quantitative generation function. (Column 3, line 22-30, the attack tree's root node value gives a quantitative measure of the security of a system in time, dollars, probability of success, or any other metric, as a function of measurements or assumptions about the attacker's resources, abilities, lawlessness, determination, etc. Furthermore, the leaf nodes of the attack tree directly illustrate the assumptions on which the security of the system is based).

Claim 29 is rejected under the same reason set forth in rejection of claim 2:

As per claim 3 Schneier discloses:

The method of Claim 1 comprising the further step of modelling countermeasures to one or more entities in the risk chain, each countermeasure being quantitatively described as a function of one or more variables. (Column 3, line 22-30, the attack tree's root node value gives a quantitative measure of the security of a system in time, dollars, probability of success, or any other metric, as a function of measurements or assumptions about the attacker's resources, abilities, lawlessness, determination, etc. Furthermore, the leaf nodes of the attack tree directly illustrate the assumptions on which the security of the system is based).

Claim 30 is rejected under the same reason set forth in rejection of claim 3:

As per claim 4 Schneier discloses:

The method of Claim 3 comprising the further step of deploying a countermeasure to an entity in such a manner so that the effect of the entity is diminished to a defined, quantitative level. (Column 22, line 45-51, when used in connection with multi-valued nodes, multiple instances of an attack tree with the same attributes, or vector-valued nodes, even more information can be obtained. For example, a cost-risk spectrum could be calculated whereby the user could choose the lowest cost system that still met an acceptable level of risk (e.g., expressed as a probability of successful attack or defense)).

Claim 31 is rejected under the same reason set forth in rejection of claim 4:

As per claim 5 Schneier discloses:

The method of claim 3 in which the or each variable describing a countermeasure determines the efficacy of that countermeasure in modifying the population of elements in an entity or influencing how one entity in the risk chain generates another entity in the risk chain. (Column 22, line 45-51, when used in connection with multi-valued nodes, multiple instances of an attack tree with the same attributes, or vector-valued nodes, even more information can be obtained. For example, a cost-risk spectrum could be calculated whereby the user could choose the lowest cost system that still met an acceptable level of risk (e.g., expressed as a probability of successful attack or defense)).

Claim 32 is rejected under the same reason set forth in rejection of claim 5:

As per claim 6 Schneier discloses:

The method of Claim 3 in which the deployment of countermeasures is quantitatively optimised. (Column 22, line 45-51, when used in connection with multi-valued nodes, multiple instances of an attack tree with the same attributes, or vector-valued nodes, even more information can be obtained. For example, a cost-risk spectrum could be calculated whereby the user could choose the lowest cost system that still met an acceptable level of risk (e.g., expressed as a probability of successful attack or defense)).

Claim 33 is rejected under the same reason set forth in rejection of claim 6:

As per claim 7 Schneier discloses:

The method of claim 1 in which the distribution of elements of an entity in a parameter is a measured distribution. (Column 3, line 22-30, the attack tree's root node value gives a quantitative measure of the security of a system in time, dollars, probability of success, or any other metric, as a

function of measurements or assumptions about the attacker's resources, abilities, lawlessness, determination, etc. Furthermore, the leaf nodes of the attack tree directly illustrate the assumptions on which the security of the system is based).

Claim 34 is rejected under the same reason set forth in rejection of claim 7:

As per claim 8 Schneier discloses:

The method of Claim 7 in which the measured distribution is a real-time measured distribution. (See column 16, line 20-30).

Claim 35 is rejected under the same reason set forth in rejection of claim 8:

As per claim 9 Schneier discloses:

The method of Claim 7 in which the measured distribution is compared to a predicted distribution, the comparison enabling the accuracy of an algorithm used to make the prediction to be improved. (Column 3, line 22-30, the attack tree's root node value gives a quantitative measure of the security of a system in time, dollars, ***probability of success***, or any other metric, as a function of measurements or assumptions about the attacker's resources, abilities, lawlessness, determination, etc. Furthermore, the leaf nodes of the attack tree directly illustrate the assumptions on which the security of the system is based).

Claim 36 is rejected under the same reason set forth in rejection of claim 9:

As per claim 10 Schneier discloses:

The method of claim 1 in which the controlled system is controlled by being dynamically altered on the basis of the modelling. (Column 6, line 5-24, while the above embodiment describes a single computer acting as computer system 200, those skilled in the art will realize that the necessary

functionality can be distributed over a plurality of computers. In one such embodiment, computer system 200 is configured in a distributed architecture, wherein the system processors and databases are housed in separate units or locations. Those skilled in the art will appreciate that an almost unlimited number of locations may be supported. Locations performing primary processing functions contain at least RAM, ROM, and a general purpose processor. Other locations need only contain sufficient storage to act as software or data servers, plus the associated processing capacity for serving the information. Each location is attached to a WAN hub having minimal processing capability and serving primarily as a communications router. This arrangement can yield a dynamic and flexible system that is less prone to catastrophic hardware failures affecting the entire system).

Claims 11, 37 and 38 are rejected under the same reason set forth in rejection of claim 10:

As per claim 12 Schneier discloses:

The method of any preceding Claim 3 in which each entity in the risk chain is an entity with substantially the properties of an entity selected from the following list of entity types: threat agents; attacks; security breaches; disruptions; damage. (Column 3, line 10-15, the database uses a tree-based structure (an attack tree) to analyze the security of a system. In one embodiment of the invention, the attack tree's root node is the goal of an attacker, the leaf nodes are attacks against that goal, and the intermediate nodes are various combinations of attacks necessary to achieve the goal).

Claim 39 is rejected under the same reason set forth in rejection of claim 12:

As per claim 13 Schneier discloses:

The method of claim 12 in which the countermeasure that modifies the threat agent entity or influences the output of that entity is an ameliorative measure. (Column 22, line 45-51, when used in connection with multi-valued nodes, multiple instances of an attack tree with the same attributes, or vector-valued nodes, even more information can be obtained. For example, a cost-risk spectrum could be

calculated whereby the user could choose the lowest cost system that still met an acceptable level of risk (e.g., expressed as a probability of successful attack or defense)).

Claim 14-16 and 40-43 are rejected under the same reason set forth in rejection of claim 13:

As per claim 17 Schneier discloses:

The method of Claim I in which the target system is a computer. (Column 4, line 50-67 and column 5, line 1-25, in these contexts, "system" is defined as any system that uses security to protect something from a specific attack. Examples include, but are not limited to: a software program that uses cryptography to protect confidentiality or to authenticate data, a encrypted telephone that allows two parties to make a confidential phone call, a physical safe, a system of writing payroll checks, a house, an entire corporate security system: a combination of computer security, physical security, personnel security, and other security measures, a telephone network, a local-area computer network, a corporate intranet, processing accounts payable, distributing payroll and so on).

Claim 18-23 and 44-50 rejected under the same reason set forth in rejection of claim 17:

As per claim 24 Schneier discloses:

The method of claim 1 in which an entity in the risk chain describes a population of one or more people who seek or otherwise obtain unauthorised access to the target system or who seek to or otherwise influence it in an unauthorised manner. (Column 1, line 6-10, the method and apparatus of the present invention relate generally to electronically analyzing the security of systems and, more particularly, to evaluating the security of an information system against unauthorized attack).

Claim 51 is rejected under the same reason set forth in rejection of claim 24:

As per claim 25 Schneier discloses:

The method of claim 1 in which an entity in the risk chain describes a population of one or more computer viruses or worms or Trojan Horses or computers. (Column 4, line 5-25, it is an object of this invention to determine the vulnerability of a system against attack).

Claim 52 is rejected under the same reason set forth in rejection of claim 25:

As per claim 26 Schneier discloses:

The method of Claim 25 in which a parameter is the age of the virus. (Abstract, line 8-11, the values of the various nodes can be Boolean or continuous, representing simple binary security attributes such as feasible/infeasible or more complicated attributes such as cost, time or probability).

Claim 53 is rejected under the same reason set forth in rejection of claim 26:

As per claim 27 Schneier discloses:

The method of claim 1 in which an entity of the risk chain describes a population of one or more fires, floods, earthquakes or other physical acts which have an impact on the target system. (Column 5, line 35-38, attackers can, of course, exploit weaknesses in safety or reliability. For example, there might be a way to steal money from a bank that only works in event of an accidental fire. Therefore, as used throughout the specification and claims, the term security shall be used to include safety and reliability considerations as well).

Claim 54 is rejected under the same reason set forth in rejection of claim 27:

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TESHOME HAILU whose telephone number is (571)270-3159. The examiner can normally be reached on Mon-Fri 7:30a.m. to 5:00p.m. EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Teshome Hailu/

Examiner, Art Unit 2434

/Kambiz Zand/
Supervisory Patent Examiner, Art Unit 2434